CLAIMS

What is claimed is:

1. A secure method of transmitting a message between a sender node and a recipient node within a network collaboration group, the sender and the recipient sharing a secret encryption key and an expected nonce value comprising:
   generating a new nonce value known to the sender;
   encrypting the message including the expected nonce value and the new nonce value, using the encryption key;
   transmitting the encrypted message from the sender to the recipient; and
   verifying, by the recipient, that the encrypted message includes the expected nonce value.

2. The method of claim 1, further comprising:
   generating a second new nonce value, known to the recipient node;
   transmitting a secure response from the recipient to the sender by repeating the method of claim 1, but this time using the second new nonce value in place of the new nonce value and using the new nonce value in place of the expected nonce value.

3. The method of claim 2, wherein the method is further repeated for one or more subsequent rounds of secure communication between the sender and the recipient, such that for each round the new nonce value of the previous message is used as the expected nonce value for the current message.

4. The method of claim 1, wherein the network collaboration group is a virtual private network.

5. The method of claim 1, wherein the sender is a key-managing master node and the recipient is a member node of the collaboration group.

6. The method of claim 1, wherein the recipient is a key-managing master node and the sender is a member node of the collaboration group.

7. The method of claim 1, wherein the method is used with a key-managing master node in order to perform an authentication process for opening a collaboration group session with a new member node.

8. The method of claim 7, wherein the method is used with the new member as the sender and the master node as the recipient, in order to initiate the authentication process.

9. The method of claim 7, wherein the method is used with the master node as the sender in order to distribute a session encryption key from the master to the member.

10. The method of claim 9, wherein a long-term password key is used as the encryption key in order to perform the authentication process, and the session key is used as the encryption key for one or more subsequent communications between the new member and the master.

11. The method of claim 10, wherein the session key is revoked by the master upon receipt of a termination message from the member.

12. The method of claim 1, further including receiving a copy of a prior message being transmitted as a replay attack, and rejecting the replay as illicit at least in part because the replay does not contain the current expected nonce value.

13. A system for managing communications within a network collaboration group, comprising:

means for generating a new nonce value;

means for incorporating an expected nonce value and the new nonce value in a message to be transmitted;

means for encrypting the message;

means for transmitting the encrypted message from a sender node of the group to a recipient node of the group; and

means for verifying, by the recipient node, that the encrypted message includes the expected nonce value.

14. The system of claim 13, wherein the means for incorporating are operable to use the new nonce value, contained in a most recent previous message from the sender to the recipient, as the expected nonce value in a current message from the recipient to the sender.

15. The system of claim 13, wherein the network collaboration group is a virtual private network.

16. A data-carrying signal for transmitting information securely between a master node and a member node of a network collaboration group, the signal being encrypted using an encryption key shared by the master and the member, the signal comprising:

the information to be transmitted;

an expected nonce value known to the master and the member; and

a new nonce value, different than the expected nonce, provided by a sender of the signal.

17. The data-carrying signal of claim 16, wherein the expected nonce value in the current transmission is obtained from the new nonce value contained in a most recent previous transmission from the sender to the recipient.

18. A method for transmitting secure messages between a master node and a member node of a network collaboration group comprising:

encrypting messages using a key shared by the master and the member, so as to protect confidentiality of the message; and

embedding a plurality of updated nonce values within said encrypted messages so as to provide verifiable integrity, authenticity, and freshness for each of said messages.